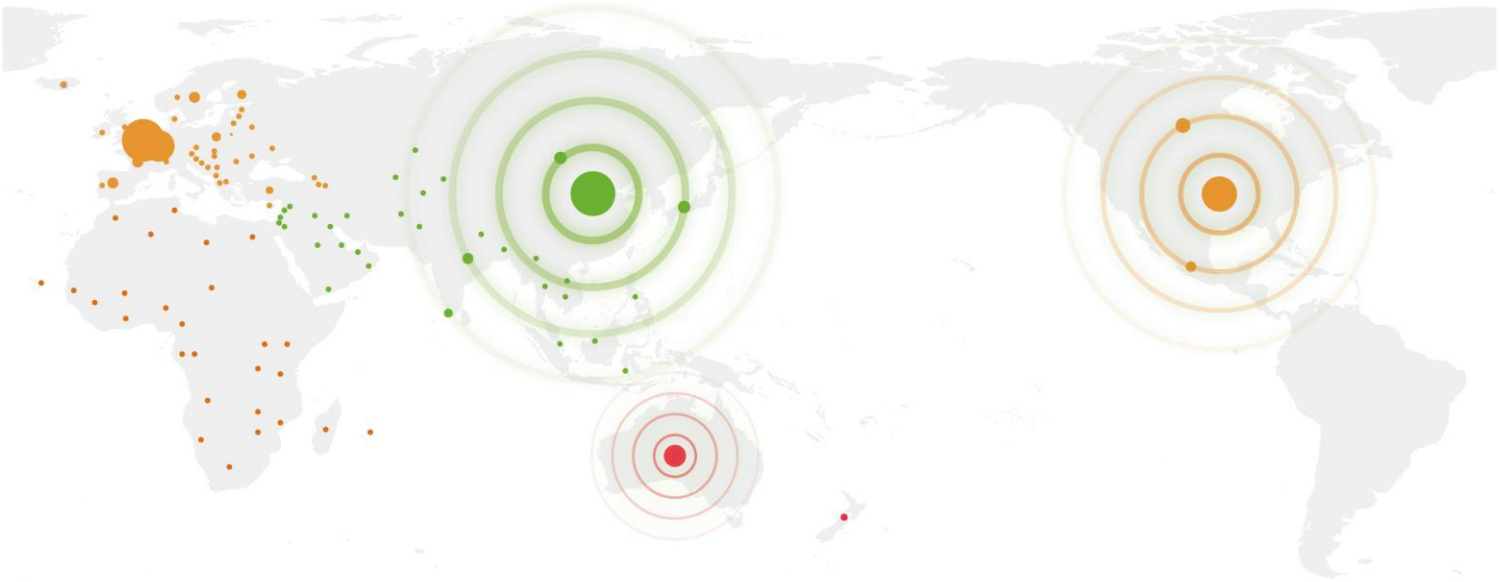
NSFOCUS

绿盟威胁情报周报

2019年第51周(12.16-12.22)



绿盟威胁情报中心(NTI)

本周热点概览

暗网情报

- 7条金融行业暗网情报，覆盖银行、证券等；
- 1条互联网行业暗网情报；

热点资讯

- Drupal修复多个漏洞；
- 2019 DDoS攻击态势报告；
- 2019年物联网安全年报；
- ECHOBOT新版本带有71个漏洞利用程序；
- APT34组织利用Poison Frog后门的攻击活动；
- Momentum僵尸网络的新攻击活动；
- 超过2.67亿个Facebook用户电话号码被公开。

一、 暗网情报

分类	发现时间	暗网交易标题
金融	2019/12/13 17:39	2019 年 5 月风车闪借 贷款审核用户数据 32W 条
金融	2019/12/13 19:39	阳光贷款 网贷借款数据 78663 条
金融	2019/12/17 14:37	广证恒生股民数据 31000 条
金融	2019/12/19 14:30	9 万 8 千条建行信用卡数据含姓名身份证号卡号手机等
金融	2019/12/19 13:39	59W 上海银行理财客户数据带手机号身份证地址等
金融	2019-12-19 19:10	12 万 8 千条交行信用卡持卡人信息含申办时的所有信息
互联网	2019/12/19 19:15	中彩网官方整站 45 万数据自动发货
金融	2019/12/19 21:47	首发金融业内部通讯录

*更多详细内容，可与绿盟科技商务人员联系或通过 csc@nsfocus.com 与我们联系

二、 热点资讯

1. Drupal 修复多个漏洞

【概述】

当地时间 12 月 18 号，Drupal 官方发布安全通告公布其核心产品中存在的多个漏洞。其中包括一个严重漏洞和三个中危漏洞。

【参考链接】

http://blog.nsfocus.net/drupal20191220/

2. 2019 DDoS 攻击态势报告

【概述】

绿盟科技发布《2019 DDoS 攻击态势报告》，2019 年 DDoS 攻击次数与 2018 年相比数增加了 30.2%，攻击总流量下降了 26.4%；1-5Gbps 小规模攻击显著增加，300Gbps 以上的大规模攻击小幅增加；平均峰值小幅增长，达 42.9Gbps，中大规模攻击的技术成熟度在逐年提高；UDP Flood、SYN Flood 和 ACK Flood 依然是 DDoS 的主要攻击手法，混合攻击在超大规模攻击中发挥重要作用；物联网设备的 DDoS 攻击参与度逐年提升；IoT 家族的漏洞利用载荷组成与 2018 年类似，主要攻击物联网智能设备，同时攻击手段增多，在攻击链上的角色出现了分工态势。

【参考链接】

https://mp.weixin.qq.com/s/fpox1B_X9Yte8992l298rA

3. 2019 年物联网安全年报

【概述】

绿盟科技发布《2019 年物联网安全年报》，报告主要内容包含对 2019 年的重大物联网安全事件进行回顾、物联网资产暴露情报分析、物联网漏洞威胁分析、物联网协议威胁分析、面对物联网终端的安全防护机制。

【参考链接】

https://mp.weixin.qq.com/s/Lo-5SXPAE0uXuAfk72RuOw

4. ECHOBOT 新版本带有 71 个漏洞利用程序

【概述】

ECHOBOT 是 Mirai 的一个变种，近期发现 ECHOBOT 最新版本带有 71 个独特漏洞利用程序，其中包含 13 个尚未被利用的漏洞，范围从 2003 年公开的 CVE 到 2019 年 12 月初最新公开漏洞，攻击针对的设备范围也很广，从常见的路由器、防火墙、IP 摄像头和管理服务器程序，到 PLC、在线支付系统、游艇控制系统等。

【参考链接】

https://unit42.paloaltonetworks.com/mirai-variant-echobot-resurfaces-with-13-previously-unexploited-vulnerabilities/

5. APT34 组织利用 Poison Frog 后门的攻击活动

【概述】

近期 APT34 组织在攻击活动中将 Poison Frog 后门伪装成合法的 Cisco AnyConnect 应

用程序。 APT34 是一个伊朗威胁组织，至少从 2014 年开始活跃，该组织主要在中东发起攻击活动。

【参考链接】

https://securelist.com/oilrigs-poison-frog/95490/

6. Momentum 僵尸网络的新攻击活动

【概述】

Momentum 针对 Linux 平台采用了各种 CPU 架构(ARM、MIPS、Intel、Motorola 68020 等)，主要目的是打开后门并接受命令以对受害目标进行 DDoS 攻击，目前已发现该勒索软件在攻击活动分发 Mirai、 Kaiten 和 Bashlite 变体。

【参考链接】

https://blog.trendmicro.com/trendlabs-security-intelligence/ddos-attacks-and-iot-exploits-new-activity-from-momentum-botnet/

7. 超过 2.67 亿个 Facebook 用户电话号码被公开

【概述】

安全研究人员在一个不安全的数据库中发现了超过 2.67 亿个 Facebook 用户 ID、电话号码和姓名，大量数据很可能是越南黑客进行的非法抓取操作或 Facebook API 滥用的结果。

【参考链接】

https://securityaffairs.co/wordpress/95404/data-breach/facebook-data-scraping.html

绿盟威胁情报中心（NTI）

绿盟威胁情报中心（NTI）依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，针对客户不同的需求场景，已经推出了云端情报查询服务（https://nti.nsfocus.com/）、互联网资产核查服务、安全设备/安全平台的威胁情报组件、客户本地威胁情报平台（NTIP）等产品及服务；为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

NSFOCUS
总部：北京市海淀区北洼路4号益泰大厦
绿盟科技（股票代码300369）

邮编：100089
电话：010-68438880
传真：010-68437328
邮箱：webadmin@nsfocus.com